## Amendments to the Claims

Claim 1 (currently amended): A method of ~~improving~~ security policy administration and enforcement ~~using a role-permission model~~ in a security system that controls access using security objects, comprising steps of:

associating each of a plurality of roles with one of the security objects, each of the security objects specifying at least one resource and for each resource, at least one action to be permitted on the resource; and

controlling access, by a plurality of subjects, to the actions on the resources using the security objects, wherein each of the subjects has been granted at least one of the roles.

~~identifying one or more groups of permitted actions on selected resources;~~

~~assigning a name to each identified group; and~~

~~associating subjects with each assigned name.~~

Claim 2 (canceled)

Claim 3 (currently amended): The method according to Claim 1, wherein at least one of the ~~selected~~ resources [[are]] is an executable ~~methods~~ method.

Claim 4 (currently amended): The method according to Claim 1, wherein at least one of the ~~selected~~ resources ~~are columns~~ is a column of a database table.

Claim 5 (currently amended): The method according to Claim 1, wherein at least one of the

~~selected~~ resources ~~are rows~~ is a row of a database table.

Claim 6 (currently amended): The method according to Claim 1, wherein at least one of the ~~selected~~ resources ~~are files~~ is a file and the permitted actions on the at least one resource are file access operations.

Claim 7 (currently amended): The method according to Claim 1, wherein at least one of the ~~selected~~ resources [[are]] is a function [[calls]] call to ~~functions~~ a function of ~~one or more~~ an executable ~~programs~~ program.

Claim 8 (currently amended): The method according to Claim 1, wherein at least one of the ~~selected~~ resources [[are]] is an Enterprise JavaBean ("EJB") ~~JavaBeans ("EJBs")~~ and the permitted actions on the at least one resource are methods on the [[EJBs]] EJB.

Claim 9 (currently amended): The method according to Claim 1, wherein at least one of the ~~selected~~ resources ~~are servlets~~ is a servlet and the permitted actions on the at least one resource are methods of the ~~servlets~~ servlet.

Claim 10 (currently amended): The method according to Claim 1, wherein at least one of the ~~selected~~ resources [[are]] is a Uniform Resource Identifier ("URI") ~~Identifiers ("URIs")~~ and the permitted actions on the at least one resource are methods which reference the [[URIs]] URI.

Claim 11 (currently amended): The method according to Claim 1, wherein at least one of the ~~selected~~ resources [[are]] is a JavaServer Page ("JSP") ~~Pages ("JSPs")~~ and the permitted actions on the at least one resource are methods referenced from the [[JSPs]] JSP.

Claim 12 (currently amended): The method according to Claim 1, wherein at least one of the ~~selected~~ resources [[are]] is any resource that is expressible to the security system and the permitted actions on the at least one resource are selected from a set of actions that are permitted on ~~those resources~~ that resource.

Claim 13 (currently amended): The method according to Claim 1, wherein the controlling step further ~~comprising~~ comprises the steps of:

receiving, from a particular one of the subjects, a ~~an access~~ request for access to a particular one of the actions on a particular one of the ~~selected~~ resources; and

permitting the requested access only if the security object created for at least one of the roles granted to the particular subject specifies the particular action on the particular resource.

~~determining one or more roles which are required for accessing the particular resource;~~

~~determining an identity of a source of the access request;~~

~~for each of the required roles, until obtaining a successful result or exhausting the required roles, determining whether the identity of the source is associated with the required role; and~~

~~authorizing access to the particular resource only if the successful result was obtained.~~

Claim 14 (canceled)

Claim 15 (currently amended): A security system for ~~improving~~ security policy administration and enforcement using security objects in a computing network ~~using a role-permission model~~, comprising:

means for associating each of a plurality of roles with one of the security objects, each of the security objects specifying at least one resource and for each resource, at least one action to be permitted on the resource; and

means for controlling access, by a plurality of subjects, to the actions on the resources using the security objects, wherein each of the subjects has been granted at least one of the roles.

~~means for identifying one or more groups of permitted actions on selected resources;~~

~~means for assigning a name to each identified group; and~~

~~means for associating subjects with each assigned name.~~

Claim 16 (currently amended): The system according to Claim 15, further comprising:

means for receiving, from a particular one of the subjects, a ~~an access~~ request for access to a particular one of the actions on a particular one of the ~~selected~~ resources; and

means for permitting the requested access only if the security object created for at least one of the roles granted to the particular subject specifies the particular action on the particular resource.

~~means for determining one or more roles which are required for accessing the particular resource;~~

~~means for determining an identity of a source of the access request;~~

~~for each of the required roles, until obtaining a successful result or exhausting the required roles, means for determining whether the identity of the source is associated with the required role; and~~

~~means for authorizing access to the particular resource only if the successful result was obtained.~~

Claim 17 (currently amended): A computer program product for ~~improving~~ security policy administration and enforcement in a security system that controls access using security objects, ~~in a computing network using a role-permission model,~~ the computer program product embodied on one or more computer readable media and comprising:

computer readable program code means for associating each of a plurality of roles with one of the security objects, each of the security objects specifying at least one resource and for each resource, at least one action to be permitted on the resource; and

computer readable program code means for controlling access, by a plurality of subjects, to the actions on the resources using the security objects, wherein each of the subjects has been granted at least one of the roles.

~~computer readable program code means for identifying one or more groups of permitted actions on selected resources;~~

~~computer readable program code means for assigning a name to each identified group; and~~

~~computer readable program code means for associating subjects with each assigned name.~~

Claim 18 (currently amended): The computer program product according to Claim 17, further comprising:

computer readable program code means for receiving, from a particular one of the subjects, a ~~an access~~ request for access to a particular one of the actions on a particular one of the ~~selected~~ resources; and

computer readable program code means for permitting the requested access only if the security object created for at least one of the roles granted to the particular subject specifies the particular action on the particular resource.

~~computer readable program code means for determining one or more roles which are required for accessing the particular resource;~~

~~computer readable program code means for determining an identity of a source of the access request;~~

~~for each of the required roles, until obtaining a successful result or exhausting the required roles, computer readable program code means for determining whether the identity of the source is associated with the required role; and~~

~~computer readable program code means for authorizing access to the particular resource only if the successful result was obtained.~~